AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF	PAGES
U	1		2

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUISITION NUMBER	5. PROJECT NUMBER *(If applicable)*
P00001	10/27/2022	1300901750-1	N/A

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE	SCD
	N65236		S0512A	C

NAVWAR-NIWC Atlantic (CHRL)
P.O. BOX 190022
North Charleston, SC 29419-9022

DCMA LOS ANGELES
6230 Van Nuys Boulevard
Van Nuys, CA 91401

8. NAME AND ADDRESS OF CONTRACTOR *(Number, street, county, State and ZIP Code)*

VSolvit LLC.
4171 Market Street, STE 2
Ventura, California 93003-8300

CODE 4L5L8 FACILITY CODE 624749359

(X) ☐ 9A. AMENDMENT OF SOLICITATION NUMBER

9B. DATED *(SEE ITEM 11)*

☒ 10A. MODIFICATION OF CONTRACT/ORDER NUMBER
N0017819D8820/N6523622F3041

10B. DATED *(SEE ITEM 13)*
09/28/2022

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to he hour and date specified in the solicitation or as amended, by one of the following me hods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

SEE SECTION G

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.

CHECK ONE	
☐	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
☐	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation data, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
☐	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
☒	D. OTHER *(Specify type of modification and authority)* FAR 43.103(a)(3); 52.204-2 Security Requirements

E. IMPORTANT: Contractor ☐ is not ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (*Organized by UCF section headings, including solicitation/contract subject matter where feasible*)

SEE PAGE 2

Except as provided herein, all terms and conditions of he document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
(b) (4), (b) (6)		Justin Maner , Contracting Officer	
15B. CONTRACTOR/OFFEROR (b) (4), (b) (6) *(Signature of person authorized to sign)*	15C. DATE SIGNED 10/27/2022	16B. UNITED STATES OF AMERICA /s/Justin Maner *(Signature of Contracting Officer)*	16C. DATE SIGNED 10/27/2022

General Information

The purpose of this modification is to incorporate the Award DD254 to the task order as Attachment 4, update PWS 13.1 with the approved subcontractors which were evaluated with the contractor's proposal, prior to task order award, and to include clause 52.244-2. All other terms and conditions remain the same.

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 67

1. CONTRACT/PURCH ORDER/AGREEMENT NO.	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMMDD)	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
N0017819D8820	N6523622F3041	2022OCT27	1300901750-1	Unrated

6. ISSUED BY CODE N65236

NAVWAR-NIWC Atlantic (CHRL)
P.O. BOX 190022
North Charleston, SC 29419-9022

7. ADMINISTERED BY *(If other than 6)* CODE S0512A

SCD: C

DCMA LOS ANGELES
6230 Van Nuys Boulevard
Van Nuys, CA 91401

8. DELIVERY FOB
- ☐ DESTINATION
- ☐ OTHER *(See Schedule if other)*

9. CONTRACTOR CODE 4L5L8 FACILITY 624749359

NAME AND ADDRESS
VSolvit LLC.
4171 Market Street, STE 2
Ventura, CA 93003-8300

10. DELIVER TO FOB POINT BY *(Date)* (YYYYMMMDD)
SEE SCHEDULE

11. X IF BUSINESS IS
- ☒ SMALL
- ☐ SMALL DISAD-VANTAGED
- ☐ WOMEN-OWNED

12. DISCOUNT TERMS
Net 30 Days WAWF

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
SEE SECTION G

14. SHIP TO CODE
SEE SECTION F

15. PAYMENT WILL BE MADE BY CODE HQ0339

DFAS Columbus Center, West Entitlement
P.O. Box 182381
Columbus, OH 43218-2381

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER
- ☒ DELIVERY/CALL — This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
- ☐ PURCHASE — Reference your ____ furnish the following on terms specified herein.

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMMDD)
VSolvit LLC.		(b) (4), (b) (6)	

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE
SEE SCHEDULE

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.

24. UNITED STATES OF AMERICA
BY: /s/Justin Maner — 10/27/2022 — CONTRACTING/ORDERING OFFICER

25. TOTAL (b) (4)

26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
- ☐ INSPECTED
- ☐ RECEIVED
- ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE (YYYYMMMDD)	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP. NO.	29. D.O. VOUCHER NO.	30. INITIALS
	☐ PARTIAL ☐ FINAL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR
f. TELEPHONE NUMBER / g. E-MAIL ADDRESS	31. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL		34. CHECK NUMBER
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT. a. DATE (YYYYMMMDD) / b. SIGNATURE AND TITLE OF CERTIFYING OFFICER			35. BILL OF LADING NO.

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED (YYYYMMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

Section C - Description/Specifications/Statement of Work

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Work under this performance-based task order will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

SHORT TITLE: MAINTENANCE FIGURE of MERIT (MFOM) SYSTEM AND SOFTWARE ENGINEERING SUPPORT

1.0 PURPOSE

1.1 SCOPE

This PWS covers systems engineering, technical, and management support services for Naval Information Warfare Center Atlantic (NIWC Atlantic) in support to the Program Executive Office for Manpower, Logistics and Business Solutions (PEO MLB), Logistics (LOG) Information Technology (IT) Services Delivery Team. This support encompasses enhancing and sustaining the Maintenance Figure of Merit (MFOM) Family of Systems (FoS) (hereinafter referred as the MFOM system) as well as transitioning and integrating MFOM's existing capabilities into PEO MLB LOG IT Services Delivery Team future Family of Systems (FoS).

NOTE: Website and e-mail addresses referenced within the PWS and Contract Data Requirements List (CDRL) forms are subject to change. For any website and e-mail address not working during time of performance, the contractor shall contact the Contracting Officer's Representative (COR) or Contracting Officer for latest website and e-mail address. An incorrect website or e-mail address does not alleviate a contractor from required reporting or access requirements.

1.2 BACKGROUND

MFOM provides near real-time material based readiness reporting to Navy maintenance communities. The MFOM system is a diverse maintenance, logistics and readiness reporting software solution with multiple components including a computing infrastructure, a cross domain solution, a multitude of configuration items, backend databases, ship/shore equipment models, communication, and messaging suites, and 16 user facing software applications that operate on classified and unclassified networks both ashore and afloat.

The PEO MLB LOG IT Services Delivery Team, the assigned Navy Program Office to manage MFOM, is executing future program and strategies to replace and integrate MFOM's capabilities into their future Family of Systems (FoS) Program.

2.0 PLACE(S) OF PERFORMANCE

2.1 GOVERNMENT FACILITIES

No Government facilities (i.e., office space or lab space) are provided on this task order. The contractor shall perform work at the contractor facility and/or temporary duty locations specified under travel.

2.1.1 Access to Government facilities

NIWC Atlantic and other Government installations have restricted access. Contractors are limited to access during certain days and times as specified in the workweek requirements of this PWS. If access to the assigned Government facility is restricted due to safety/security exercise, an Executive Order, or an administrative leave determination applying to the local activity (e.g., inclement weather), the contractor, in agreement with the COR, shall make alternative work arrangements. The contractor shall adjust work schedule, work at an alternate location, or if alternate work arrangements cannot be accommodated, the contractor shall notify the COR of the inability to access the assigned facility prior to charging their time to the task order as direct cost provided such charges are consistent with the contractor's accounting practices. The ability to work at an alternate location that is not a Government or contractor facility site is dependent on the contractor having an alternative work site agreement with the employee. The ability to work at an alternate location may not be an option for certain support services.

2.1.2 Training Requirements and Exercise Support

Contractor personnel working full-time or partially at a Government facility shall complete all applicable training requirements as specified under Mandatory Training, PWS Para 8.0. Contractor personnel may also be required to participate in safety, security (e.g., Anti-Terrorism Force Protection (AT/FP)), and operational training exercises (possibly two per year). Applicable contractor personnel shall support and participate in the training exercise which may include role-playing and reacting to exercise injects based on the situation or exercise objectives.

2.1.3 Emergency Management at Government Installations

During emergency situations including health (e.g., COVID-19 pandemic) and weather related circumstances, contractor personnel with scheduled access to a Government installation shall coordinate with the COR prior to reporting to their Government worksite. Access will be in accordance with the latest Government installation requirements and restrictions. The contractor shall identify with the COR if certain personnel are designated mission essential and determine the work expectations during the emergency period of performance. Depending on the type of support, working from an alternative worksite may or may not be allowed.

2.2 CONTRACTOR FACILITIES

A significant portion of work issued under this task order requires close liaison with the Government. The contractor shall be prepared to establish a local facility within a thirty (30)-mile radius of NIWC Atlantic Norfolk facility located at 9440 Maryland Avenue, Bldg. Z133, Norfolk, VA 23511. The contractor shall be capable of quickly interfacing with the secure labs located at NIWC Atlantic. The contractor's facility is not necessarily for the exclusive use of this task order and can be utilized on a shared basis. The contractor shall meet all facility requirements within 30 days after task order award. The contractor shall ensure facility includes space for offices, conference rooms, lab work, and a staging area for materials

and equipment.

2.3 ALTERNATE WORK LOCATIONS

The ability to provide support from an alternate location (includes working from an employee's residence or other non-Government facility) is dependent on the type of support required, the contractor employee's ability and trustworthiness, and the company's employment policy. Allowing work to be performed at an alternate location is not an option for all positions and personnel. The ultimate decision to allow work performed at an alternate work location will be determined by the COR. If alternate work locations are allowed, the company shall have defined criteria addressing the minimum requirement to have continuous, secure internet connectivity. Each applicable contractor employee shall have an established signed telework agreement between the company and employee. For each contractor employee proposed to work at an alternate location, the contractor shall submit a written request and justification to the COR with a copy of the applicable employee's signed telework agreement which becomes part of the COR files. If the requirements for teleworking and/or alternate work locations are not outlined/specified in the employee agreement documentation, the contractor shall include a copy of those requirements with the signed employee agreement. Working at an alternative location shall not adversely affect the response time required in support of the task order. The Government reserves the right to disallow any billable hours by contractor employees working at an alternative work location without obtaining prior Government approval. The Government reserves the right to discontinue the ability to work from an alternate location at any time without cause. The inability of a contractor to respond to the requirements of the task order due to telework conditions will be negatively reflected in the Contractor Performance Assessment Reporting System (CPARS). The contractor shall utilize the Government site or Client site (vice contractor site) overhead labor rate for personnel working from their residence unless their Accounting System requires a different billing structure.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list non-personal services tasks that will be required throughout this task order. The contractor shall provide necessary resources with knowledge and experience as cited in the personal qualification requirement to support the listed tasks. The contractor shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) that do not include performance of inherently Government functions. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

3.1 PROJECT MANAGEMENT SUPPORT

The contractor shall provide project management (PM) services to support PEO MLB, LOG IT Services Delivery Team in maintaining, enhancing, and sustaining MFOM.

3.1.1 Program Support

The contractor shall provide program support services for planning, organizing, and managing resources to bring about the successful execution of specific program/project goals and objectives as defined in this PWS. The primary objective of this task is to achieve all of the project goals and objectives while adhering to specific project constraints (scope, quality, schedule, and cost). The contractor shall apply standards, principles, and techniques of project management to monitor, control, and direct completion of all requirements, from receipt and initiation through planning, scheduling, execution, monitoring, transition, and closure. The contractor shall document and update its progress on completing tasking in the Task Order Status Report (TOSR) (CDRL T001) that is detailed in Section 5 of this PWS. Contractor shall:

1. Plan, schedule, facilitate, and document meetings
2. Provide Subject Matter Expertise (SME) to support to the Government
3. Respond to the Government's status reporting and data call requests
4. Assist the Government with program planning
5. Record, track, and manage action items
6. Conduct analysis and develop recommended Courses of Action (COAs)
7. Develop strategic initiatives to enhance performance and capabilities
8. Develop, collect, and report performance metrics
9. Provide technical writing and editing support to enhance documentation

3.1.2 Schedule Management Support

The contractor shall coordinate with the Government to develop an approach, and define the associated artifacts, to manage the schedule requirements associated with this PWS. The contractor shall tailor this plan to the overall MFOM execution methodology and document this approach in the Cost and Schedule Milestone Plan (CDRL T002) as outlined in Section 5 of this PWS. The contractor shall provide monthly updates to the defined schedule artifacts as part of both the Task Order Status Report (TOSR) (CDRL T001) and monthly Program Management Review (PMRs) (CDRL T003). The contractor shall use this plan to:

1. Manage planned events and project milestones
2. Manage task due dates and constraints
3. Manage task order deliverables
4. Manage internal and external dependencies
5. Identify and report schedule risk, issues, and variances

6. Identify recommendations and corrective actions to be implemented to mitigate risk

7. Integrate schedule data and artifacts with other Government plans and schedule artifacts

3.1.3 Cost Management Support

The contractor shall coordinate with the Government to develop an approach, and define the associated artifacts, to manage the cost associated with this task order. The contractor shall tailor this plan to the overall MFOM Program methodology and document this approach and associated artifacts in the Cost and Schedule Milestone Plan (CDRL T002). The contractor shall provide a Contract Funds Status Report (CDRL T004) and discuss cost performance and results during the monthly Program Management Reviews (CDRL T003). The contractor shall include the following cost management elements in its approach and cost management artifacts:

1. Expended costs by month

2. Projected costs by month

3. Estimates and Variances at Completion

4. Actual and planned labor hours by month

3.1.4 Risk Management Support

The contractor shall provide support by utilizing the risk parameters identified in the Government MFOM IPT Project Management Plan and assist in identifying and documenting all relevant risks to include mitigation strategies and contingency plans for risks, when required. The contractor shall report the total risks (including mitigation and contingency), exposure trends, and risk composite summaries to the Government during the monthly PMRs (CDRL T003) as well as include updates to risk as part of the Task Order Status Report (TOSR) (CDRL T001).

3.1.5 Project Management Reviews (PMR)

The contractor shall coordinate, prepare, and conduct monthly PMRs (CDRL T003). The purpose of the PMRs is to ensure both the contractor and the Government have a mutual understanding of the progress and status of tasking with this PWS.

3.2 TECHNICAL AND ENGINEERING SUPPORT

The contractor shall provide technical and engineering support necessary to enhance, improve, and sustain MFOM's existing capabilities. Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended work week (EWW) may be required to provide this support. The contractor shall execute this support in accordance with the Government's Software Development Lifecycle (SDLC) Guide. The SDLC is based on the Agile software development methodology and processes that have been approved and directed by PEO MLB LOG IT Services Delivery Team. The contractor shall meet evolving requirements while leveraging Agile best practices in software development, and with an extensible infrastructure and robust communication between the product sponsor and the project team. Additionally, the contractor shall provide this support using the engineering toolsets implemented and provided by the Government as defined in Attachment 2 of this PWS.

3.2.1 Technical Support

The contractor shall provide technical support across a broad range of Program tasking to assist the Government with enhancing, sustaining, and maintaining the MFOM system. Contractor shall:

1. Conduct technical assessments and develop recommended Courses of Action (COA)

2. Respond to technical data calls

3. Provide technical MFOM Subject Matter Expertise (SME) to support working groups and meetings

4. Coordinate technical exchanges with external organizations and systems that impact MFOM

5. Troubleshoot and analyze system trouble tickets, outages, and performance issues, may require EWW

6. Support Alteration Installation Team (AIT) resources while completing shipboard installations, may require EWW

3.2.2 Requirements Engineering and Management Support

The contractor shall provide requirements engineering and management support for the evolution of existing MFOM capabilities, systems, and external systems interfaces. The contractor shall maintain and update MFOM's requirements repository.

The contractor shall implement and support a change management process that allows MFOM stakeholders to request changes to the MFOM baseline while identifying requirements that are being impacted. The contractor shall analyze the requested changes and provide technical recommendations and assessments for implementing the changes. The contractor shall maintain traceability of the Change Request (CR) to MFOM's documented requirements as well as provide a Requirements Traceability Matrix (RTM) (CDRL T 005) for each MFOM baseline release. The contractor shall analyze and decompose MFOM CRs into user stories. The contractor shall manage CRs, and their associated user stories, throughout their Agile development lifecycle while showing traceability between system requirements and capabilities. Contractor shall:

1. Elicit and document stakeholder requirements through storyboarding, user interface mock-ups, and other artifacts

2. Define acceptance criteria

3. Identify interdependencies

4. Identify business values

5. Define the required testing approach

6. Assess and estimate the level of effort and complexity

7. Develop and maintain traceability to requirements and capabilities

8. Document, update, and report CRs, user stories, and their associated artifacts

9. Provide management reports for CR status and progress

10. Assign requirements to the Release Roadmap (CDRL T020) based on stakeholder priorities

3.2.3 Solution Architecture Support

The contractor shall develop, enhance, document, and maintain a solution architecture that satisfies the MFOM solution's requirements using applicable frameworks and processes including the Department of Defense Architecture Framework (DoDAF) and Model-Based Systems Engineering (MBSE).

The contractor shall encapsulate and define areas of the solution expressed as a set of separate problems of manageable, conceptual, and ultimately realizable proportions. The contractor shall identify and explore one or more implementation strategies at a level of detail consistent with the system's technical requirements and risks. The contractor shall:

1. Establish, update, maintain, and document architectural design baselines and associated architecture artifacts (CDRL T006)

2. Manage traceability between the design baselines to system requirements and capabilities

3. Develop, update, and maintain internal and external system interface requirements and specifications

4. Assess solution architecture changes to support CRs

The contractor shall evaluate MFOM's existing architecture and identity opportunities to reduce the lifecycle management complexity as well as to support the transitioning and integration with future maintenance programs and systems. The contractor shall:

1. Implement a microservice based architecture

2. Implement representational state transfer (RESTful) web services

3. Implement containerization technologies

4. Transition infrastructure platforms to authorized DoD cloud hosting services

5. Update MFOM underpinning commercial off the shelf (COTS) technologies to updated vendor releases and capabilities

3.2.4 Infrastructure Engineering

The contractor shall provide engineering expertise to support the development of architectural and technical designs for MFOM's IT infrastructure. This infrastructure includes the infrastructure platforms defined in Attachment 2 of this PWS and includes development, test, training, pre-production, and production environments. The contractor shall:

1. Design and enhance computing server architecture

2. Derive technical requirements

3. Define server capacity specifications for compute processing, memory, and storage

4. Develop and enhance operating system baselines

5. Develop and enhance server virtualization baselines

6. Develop and enhance platform services baselines

7. Design scalability, redundancy, and disaster recovery infrastructure to ensure uninterruptable access while protecting data integrity

3.2.5 Configuration Management (CM) Support

The contractor shall implement a disciplined process that provides a common and structured approach necessary to minimize variation of establishing and maintaining consistency across MFOM's requirements, performance, physical attributes and its design and operational information while applying management and planning, configuration identification, configuration control, configuration status accounting, configuration verification and audit functions in a closed-loop process throughout its life cycle. The contractor shall:

1. Develop, establish, document, and execute managed and repeatable CM processes across the MFOM's lifecycle in a Configuration Management Plan (CDRL T007)

2. Select, define, document, baseline MFOM's product and service attributes and assigning unique identifiers to processes, products and services, and associated configuration information throughout the lifecycle

3. Ensure and implement a consistent systematic change process that establishes and maintains control of MFOM's configuration baselines and changes to processes, products, and services are properly identified, recorded, evaluated, approved, or disapproved and incorporated and verified as appropriate

4. Establish, maintain, and report process, product, and service information to ensure that MFOM's configurations can be determined, recorded, safeguarded and validated to ensure accuracy throughout the life cycle

5. Review and evaluate MFOM's processes, products, and services to validate compliance and ensuring integrity with requirements

6. Manage, monitor, store MFOM's management and technical configuration information

7. Ensure that all supporting commercial technologies integrated into the MFOM baselines are registered in Navy's Application and Database Management System (DADMS) and are Functional Area Manager (FAM) approved

3.2.6 Data Science

The contractor shall provide Navy maintenance domain, mathematical, algorithms and technical expertise to analyze structured and unstructured data to extract knowledge and information on maintenance data obtained from the MFOM system and other Navy maintenance data sets. The contactor shall collect, prepare, transform, and analyze maintenance data as well as present the results of its analysis to the Government (CDRL T011). The contactor shall support the development and integration of data science based algorithms into MFOM's solution architecture to enhance readiness reporting and predictive maintenance capabilities. The contractor shall apply various data science techniques such as regression, decision trees, clustering, and machine learning using various data science programming and scripting languages and frameworks including or similar to PEO MLB LOG IT Services Delivery Team's future Integrated Data Environment (IDE).

3.3 APPLICATION PRODUCT MANAGEMENT SUPPORT

The contractor shall provide application product management support to ensure that MFOM is a sustainable system that meets stakeholder requirements. The contractor shall execute this support in accordance with the Government's SDLC Guide which is based on the Agile software development methodology and processes. The contractor shall facilitate collaboration, meetings, and discussions across MFOM's broad stakeholder community to elicit, identify and define stakeholder needs to improve, enhance, or correct MFOM's capabilities and requirements. The contractor shall support stakeholders and their respective organizations to understand, embrace, and adopt Agile methodologies, processes, and culture. The contractor shall also facilitate the prioritization process of these needs across the stakeholders and develop a MFOM product vision, an Agile backlog, and Release Roadmap (CDRL T020) to meet these needs using the engineering tools defined in Attachment 2. The contractor shall document solution changes using a Change Request (CR) process. The contractor shall conduct planning to develop and deliver capabilities based on the product vision and Release Roadmaps (CDRL T020) incrementally (thereinafter referred to as Increments). For each defined Increment, the contractor shall schedule and facilitate a planning event that integrates the MFOM stakeholders to collaboratively develop an executable plan that is endorsed across the MFOM stakeholder community. The contractor shall document the results of these events in a Planning Increment Report (CDRL T009).

Within a defined Increment, the contractor shall execute the work required to complete the Increment plan using fixed time-boxed periods to execute the planned work (thereinafter referred to as Iterations). The contractor shall decompose the Increment plan to the Iterations that are part of the Increment.

The contractor shall facilitate the planning and assignment of individual requirements and user stories targeted for development during an Iteration across the MFOM stakeholder community. The contractor shall focus this planning based on the prioritized capabilities for the Increment. At the completion of an Iteration, the contractor shall conduct an Iteration review to the MFOM stakeholder community that summarizes work accomplished for that Iteration, demonstrate work completed, as well as communicate the planned worked for the next Iteration. The contractor shall also include risks, issues, impediments, and performance metrics. The contractor shall document the Iteration review results in an Iteration Review Report (CDRL T010).

The contractor shall support release management activities necessary to deliver and deploy to production capabilities that have completed development based on the defined Release Roadmap (CDRL T020). The contractor shall deliver software baselines and supporting artifacts in accordance with the Government's Software Development Lifecycle Guide. Software baselines and supporting artifacts including:

1. Source code (CDRL T011)

2. Binary code

3. Requirements Traceability Matrix (RTM) (CDRL T005)

4. Automated/Manual Test Cases

5. Iteration Testing Results

6. Installation Deployment Scripts

7. Source code static code security results

8. System Operational Verification Test (SOVT) Procedures

9. System Installation Guides

10. Systems Administration Guide

11. Release Notes

12. If necessary, changes and enhancements to the Software Documentation/Programmer's Guide (CDRL T012)

Upon completion of the delivering the software baselines, the contractor shall support the deployment of the baseline to Production. The contractor shall:

1. Support pre-production testing

2. Support communications to stakeholders on release baseline changes and capabilities

3. Analyze and assess issues discovered during pre-production testing

4. Correct release defects

5. Support and resolve issues with deploying releases into the production environment

3.4 SOFTWARE ENGINEERING SUPPORT

Software engineering includes the design, development, and documentation of software to support a specific government requirement. The contractor shall utilize certified software and computer personnel. The contractor (prime and/or subcontractor) that is responsible for leading software development efforts shall define a software development approach appropriate for the computer software effort to be performed under each task. The contractor shall document the approach in a Software Development Plan (SDP) (CDRL T013). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort. The contractor shall develop one SDP to support the unique task order software requirements. At a minimum, the contractor shall ensure the SDP meets the criteria specified in the CDRL DD1423 using ISO/IEC/IEEE 12207:2017 and the PWS tasking.

As defined in DFARS 252.227-7014, the contractor shall design, develop and deliver computer software including computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled.

The contractor shall execute the work using the programming and scripting languages reflected in PWS Attachment 2, Section 1.5.

The contractor shall execute the work using the engineering toolsets implemented and provided by the Government as reflected in PWS Attachment 2, Section 1.4.

The contractor shall reference and ensure the SDP is consistent with the Government's Software Development Life Cycle Guide which is based on the Agile software development methodology and processes. The contractor shall execute software development consistent with the defined Increments and Iterations defined in section 3.3 of this PWS. The contractor shall decompose requirements and define user stories that are planned for an Iteration to sufficient level of detail to support the development. The contractor shall:

1. Develop end user storyboard or screen wireframes for user interactions
2. Develop structural and behavior diagrams
3. Define acceptance criteria and corresponding testing approach
4. Define the level of effort to complete development effort
5. Ensure and validate requirement traceability
6. Update and enhance architecture artifacts (CDRL T006)

The contractor shall implement and execute software development using Development Security Operations (DEVSECOPS) processes and tooling to reduce software delivery lifecycle and ensure software quality. The contractor shall implement:

1. Source code management
2. Continuous integration build management
3. Software baseline and artifact management
4. Source code quality, complexity, and security assessments
5. Software testing
6. Software packaging, integration, and deployment management

Upon the completion of development, the contractor shall deliver software and supporting artifacts to the Government electronically to the Government repositories. Software and supporting artifacts include or are similar to:

1. Source code (CDRL T011)
2. Binary code
3. Requirements Traceability Matrix (RTM) (CDRL T005)
4. Automated/Manual Test Cases
5. Iteration Testing Results
6. Installation Deployment Scripts
7. Source code static code security results
8. Release notes
9. If necessary, changes and enhancements to:
    a. Software Documentation/Programmer's Guide (CDRL T012)
    b. System Operational Verification Test (SOVT) Procedures
    c. System Installation Guides
    d. Systems Administration Guide
    e. Architecture artifacts (CDRL T006)

3.5 CYBERSECURITY AND INFORMATION ASSURANCE SUPPORT

The contractor shall provide cybersecurity and Information Assurance (IA) support to the MFOM program to assure information and manage risk for the use, processing, storage, and transmission of information. The contractor shall assure the integrity, availability, authenticity, non-repudiation and confidentiality of user data. The contractor shall:

1. Analyze cybersecurity policies and requirements and derive solution requirements

2. Implement cybersecurity risk reduction throughout the solution lifecycle

3. Assess security risks of MFOM baselines prior to release

4. Execute static code security scans and remediate identified vulnerabilities

5. Execute cybersecurity scans such as Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP) and remediating identified vulnerabilitie

6. Assess and respond to information assurance vulnerability alerts (IAVA)

7. Execute the Risk Management Framework (RMF) processes and requirements to establish and maintain accreditations

3.6 TRANSITION-IN/OUT

The Government anticipates 60-90 calendar days for transition-in and transition out. The objective of this task is to provide migration of current activities performed by the incumbent Contractor to a successor Contractor and may require redesigning the current approaches to align with requirements. Transition entails the transfer of and assumption of responsibility for project documentation, resources, assets, and performance. The Transition tasks will ensure uninterrupted operations and sustainment support at the end of the period of performance. At the direction of the Government, the Contractor shall provide accountability for the transition of all on-going activities performed by the incumbent Contractor to a successor Contractor or to the Government or to any supporting third party entities. Transition entails the transfer of responsibility for project documentation, resources, assets, and performance to the designated party. It also includes the implementation and readiness of capabilities necessary for all aspects of performance redesign of current technical and management approaches, assumption of audit reviews and readiness all without disruption in schedule, increased costs, degradation to performance, need for increased Government oversight, or likelihood of unsuccessful performance. The Contractor shall document meetings, attendance of individuals, and development of standard operating procedures as appropriate.

3.6.1 Transition Planning and Management

The Contractor shall develop and execute a Transition Plan (CDRL T015) to ensure an effective, orderly and efficient execution of both transitioning in and out for either all or a part of the services under this Task Order as directed by the Government. Transition activities include planning, discovery, and programmatic functions (e.g., Contract Management, Human Resource Management, and Quality Assurance) necessary for establishing effective knowledge transfer. Throughout the transition period, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission.

3.6 2 Transition Activity

The Contractor shall transition all active tasks at the time of the transition and all associated system documentation and tools updated to represent the current baseline implementation. Specifically, the Contractor shall:

1. Execute transition activities to ensure continuity of services, minimize any decreases in productivity, prevent degradation of services, and prevent negative impacts to the continuity of care during the transition period

2. Provide knowledge transfer, support successor job shadowing, training, and other activities in order to successfully transition operation of services

3. Transfer software licenses to the Government

4. Deliver all training documentation requested by the Government

5. Transfer documents, badges, and CACs

6. Identify and transfer or destroy any classified materials or information IAW Government Security Officer instructions

7. Deliver all technical data, computer software, and computer software documentation generated in the performance of this contract pursuant to DFARS 252.227-7027 (http://www.acq.osd.mil/dpap/dars/dfars/html/current/252227.htm)

8. Deliver all commercial and non-commercial technical data, computer software, and computer software documentation not generated in performance of this Task Order that is necessary, as determined by the Government at its sole discretion, to operate and sustain MFOM throughout its lifecycle

9. If requested by the Government, export and deliver all data content with context (e.g., schemas, data format, data descriptions, and metadata) in a Government approved common standard electronic machine-readable format

10. Provide transition progress updates as part of the Task Order Status Report (CDRL T001) and during the Monthly Program Reviews (CDRL T003)

11. Transfer service responsibility at the end of the transition timeframe, upon which the successor Contractor shall assume responsibility for operational, technical, and financial performance

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

The contractor shall adhere to the following requirements when the IT support services and/or supply are applicable to the requirement:

4.1.1 Ensure that no production systems are operational on any research, development, test and evaluation (RDT&E) network.

4.1.2 Follow DoDI 8510.01 when deploying, integrating, and implementing IT capabilities.

4.1.3 Migrate all Navy Ashore production systems to the Navy, Marine Corps Intranet (NMCI) environment where available.

4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3C and DoDI 8510.01 prior to integration and implementation of IT solutions or systems.

4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on task order in the Department of Defense IT Portfolio Registry (DITPR)-DON.

4.1.7 Ensure all IT products and services recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, Title 36 Code of Federal Regulations Part 1194 – Electronic and Information Technology Accessibility Standards unless otherwise exempt in accordance with the latest regulation.

4.1.8 Only perform work specified within the limitations of the basic contract and task order.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors recommending or purchasing commercial software products, hardware, and related services that support Navy or DoD programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

4.2.1 DoN Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program

The contractor shall not purchase software or software licenses in support of DoN or DoD programs on this task order.

4.2.2 DoN Application and Database Management System (DADMS)

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. The RDT&E network does not provide continuous support to operational entities. The contractor shall ensure that any system achieving operation fleet readiness and support is removed from the RDT&E environment and hosted on the respective enterprise solution as required. The contractor shall ensure any systems or applications integrated, installed, or operated on the RDT&E network must be in accordance with DADMS and/or DITPR-DON registration policies. Exemptions to this policy can apply as specified by higher directives Exemptions on systems that remain on the RDT&E are normally systems that support the RDT&E or have to be on the RDT&E to achieve their target of support.

4.2.3 Cybersecurity/Computer Security Requirements

The contractor shall ensure that all products recommended and/or procured that impact cybersecurity or Information Assurance (IA) shall be selected from the National Information Assurance Partnership (NIAP) Validated Products List. The contractor shall ensure the products chosen are based on the appropriate NIAP-approved Protection Profile (PP) for the network involved, and are utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. The contractor shall store all product information and have it available for government review at any time.

4.2.4 Supply Chain Risk Management

“Covered item of supply” (e.g., software, processor, etc.) is any information technology item that is purchased for inclusion in a “covered system” (i.e., national security systems). In accordance with DFARS 252.239-7018, the contractor shall have mechanisms in place to effectively monitor the supply chain for critical components, understands how supply chain risk can be introduced through those components, and shall have implemented or plans to implement countermeasures to mitigate the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

4.3. SOFTWARE DEVELOPMENT/MODERNIZATION AND HOSTING

The contractor shall ensure all programs utilizing this task order for software development/ modernization (DEV/MOD) including the development of IT tools to automate NIWC Atlantic

business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate NIWC Atlantic business processes unless specifically tasked within the task order. The contractor shall ensure IT tools developed to automate NIWC Atlantic business processes will be delivered with Software Documentation/Programmer's Guide (CDRL T012) and Source Code (CDRL T011) to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to task order award. In accordance with DITPR-DON policy, contractor shall ensure all applicable software is part of the Investment Review Board (IRB) approved list. At a minimum the Government shall have Government Purpose Rights in any computer software and technical data developed under the task order.

4.4 CYBERSECURITY SUPPORT

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

The contractor shall have the appropriate Non-Secure Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) access required to support the Cybersecurity and Information Assurance requirements for the MFOM system (Reference System Details, Attachment #2) and future PEO MLB LOG IT Services Delivery Team's FoS.

4.4.1 Cyber IT and Cybersecurity Personnel

4.4.1.1 The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M and subsequent manual [DoD 8140] when applicable prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

4.4.1.2 Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in Para 8.2.2.4(b).

4.4.1.3 Contractor personnel with privileged access shall have a favorably adjudicated Tier 5 background investigation and acknowledge special responsibilities with a Privileged Access Agreement (PAA) in accordance with SECNAVINST 5239.20A.

4.4.2 Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in Para 4.2 2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

4.4.3 Cybersecurity Workforce (CSWF) Report

In accordance with DFARS 252.239-7001 and DoD 8570.01-M, the contractor shall identify cybersecurity personnel, also known as CSWF and Cyber IT workforce personnel. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL T014) identifying CSWF individuals who are IA trained and certified. Utilizing the format provided in the CSWF Report (CDRL T014) Attachment 1 of Exhibit A, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Although the minimum frequency of reporting is monthly, the COR can require additional updates at any time. Contractor shall verify with the COR or other Government representative the proper labor category CSWF designation and certification requirements. The primary point of contact (POC) for all related CSWF questions is the Command CSWF Program Manager (PM) in the office of the NIWC Atlantic Information Systems Security Manager (ISSM).

4.4.4 Cybersecurity Workforce (CSWF) Designation

CSWF contractor personnel shall perform cybersecurity functions. In accordance with DoD 8570.01-M Information Assurance Workforce Improvement Program Manual, the CSWF is comprised of the following categories: IA Technical (IAT) and IA Management (IAM)); and specialties: Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs). Based on the IA function provided by the individual, an IA designator is assigned that references an IA category or specialty. The contractor shall have the following quantity of CSWF personnel meeting IA Designator and IA Level/Position requirements:

Labor Category	**Quantity Personnel**	**IA Designator**	**IA Level/Position**	**IA Duty Hours**		
				Primary (=25 hrs)	**Additional (15-24 hrs)**	**Embedded (1-14 hrs)**
Engineer/Scientist Intern	1	IAT	Level 1			X

Labor Category	Quantity Personnel	IA Designator	IA Level/Position	IA Duty Hours		
				Primary (=25 hrs)	Additional (15-24 hrs)	Embedded (1-14 hrs)
Engineer/Scientist 1	1	IAT	Level 1			X
Engineer/Scientist 2	6	IAT	Level 1			X
Engineer/Scientist 3	14	IAT	Level 1			X
Engineer/Scientist 4	9	IAT	Level 1			X
Engineer/Scientist 4	2	IAT	Level 3	X		
Engineer/Scientist 5	10	IAT	Level 1			X
Engineer/Scientist 5	2	IAT	Level 3	X		
Management Consultant (Senior)	1	IAT	Level 1			X
Subject Matter Expert (SME) 1	1	IAT	Level 1			X
Subject Matter Expert (SME) 2	1	IAT	Level 1			X
Subject Matter Expert (SME) 3	2	IAT	Level 1			X
Subject Matter Expert (SME) 4	1	IAT	Level 1			X
Subject Matter Expert (SME) 5	15	IAT	Level 1			X
Technical Analyst 2	8	IAT	Level 1			X
Technical Analyst 3	8	IAT	Level 1			X
Technical Analyst 3	2	IAT	Level 3	X		
Technical Analyst 4	10	IAT	Level 1			X

5.0 TASK ORDER ADMINISTRATION

Administration of the work being performed is required; it provides the Government a means for task order management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government's requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACTOR LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and COR. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all Government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for task order performance and be available to support emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate periodic meetings with the COR.

5.2 CONTRACT MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day including business and non-business hours in order to facilitate a timely task order response or modification in particular during urgent requirements.

5.2.1 Task order Administration & Documentation

Various types of administration documents are required throughout the life of the task order. At a minimum, the contractor shall provide the following documentation:

5.2.1.1 Task Order Status Report (TOSR) -- The contractor shall develop a Task Order Status Report (TOSR) (CDRL T001) and submit it monthly; the initial report is due at least 30 days after task order award and on the 10th of each month for those months the task order is active. The prime contractor shall be responsible for collecting, integrating, and reporting any subcontractor reports. This CDRL includes the completion of applicable attachment(s) as cited in the DD Form 1423. The contractor shall deliver the TOSR in an editable format; see applicable DD Form 1423 for additional reporting details and distribution instructions.

5.2.1.2 Ad-hoc Status Report/Data Calls – the contractor shall develop and submit a Data Call Report (CDRL T016) which is e-mailed to the COR within 24-48 hours of the request. The contractor shall ensure all information provided is the most current. Cost and funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum, the contractor shall include in the data call the following items and data:

1. Percentage of work completed
2. Percentage of funds expended
3. Updates to the POA&M and narratives to explain any variances
4. List of personnel (by location, security clearance, quantity)
5. Most current GFP and/or contractor acquired Property (CAP) listing

5.2.2 Closeout Report

The contractor shall develop a task order Closeout Report (CDRL T017) and submit it no later than 15 days before the task order completion date to allow for any corrective actions. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontracting information, if applicable. See corresponding DD Form 1423 for additional reporting details and distribution instructions. The contractor shall ensure with the COR no corrective action is identified, and if corrective action is necessary, the contractor shall rectify issue prior to the end of task order performance period.

5.2.3 WAWF/PIEE Invoicing Notification and Support Documentation

Pursuant to DFARS 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Wide Area Work Flow (WAWF) application (part of the Procurement Integrated Enterprise Environment (PIEE) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. The contractor shall provide e-mail notification to the COR when payment requests are submitted to the WAWF/PIEE and the contractor shall include cost back–up documentation (e.g., delivery receipts, time sheets, & material/travel costs, etc.) to the invoice in WAWF/PIEE. When requested by the COR, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL A018) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.2.4 Electronic Cost Reporting and Financial Tracking (eCRAFT)

The contractor shall complete an Electronic Cost Reporting and Financial Tracking (eCRAFT) Report (CDRL T019) and submit the report on the day and for the same timeframe as when the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. The amounts reported in eCRAFT Periodic Reporting Utility (EPRU) spreadsheet shall be the same reported in WAWF. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination. See applicable task order Attachment 6 for eCRAFT Crosswalk and DD Form 1423 for reporting details and upload instructions.

5.3 CONTRACT PERFORMANCE MANAGEMENT

Contractor performance standards and requirements are outlined in the task order QASP. The ability of a contractor to perform to the outlined standards and requirement will be captured in the Contractor Performance Assessment Reporting System (CPARS). In support of tracking contractor performance, the contractor shall provide the following documents: Cost and Schedule Milestone Plan (CDRL T002) submitted 10 days after task order award and CPARS Draft Approval Document (CDAD) Report (CDRL T008) submitted monthly.

5.4 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this task order does not require Earned Value Management (EVM) implementation due to the majority of efforts on this task order is non-scheduled based (i.e., level of effort) and does not lend itself to meaningful EVM information. In lieu of an EVM system, the contractor shall develop and maintain a Contract Funds Status Report (CDRL T004) to help track cost expenditures against performance.

6.0 DOCUMENTATION AND DELIVERABLES

6.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

The following listing identifies the data item deliverables required under this task order and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under this task order. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs. The contractor shall not develop any CDRL classified TOP SECRET with Sensitive Compartmented Information (SCI).

Unless otherwise specified, dates are calendar days; one week equals 7 calendar days; 1 day equals 24 hours; and a 24-hour time period is consecutive hours that is exclusive of non-workweek days.

6.1.1 Administrative CDRL

The following table lists all required administrative data deliverables, CDRLs, applicable to this task:

CDRL #	Deliverable Title	PWS Reference Para	Frequency	Date Due	Security Classification (up to S/TS or unclassified)
T001	Task Order Status Report (TOSR)	3.1.1, 3.1.2, 3.1.4, 3.6.2, 5.2.1.1, 5.2.4, 8.1.2, 8.2.3.1, 10.0, 10.3.3, 10.3.3.2, 10.3.3.3	MTHLY	30 days after task order award (DATO) and monthly on the 10th	Unclassified
T002	Cost and Schedule Milestone Plan	3.1.2 3.1.3 5.3	ONE/R	NLT 10 DATO; revision NLT 7 days after receipt of Govt review	Unclassified
T004	Contract Funds Status Report (CFSR)	3.1.3 5.4	MTHLY	10th of Each Month	Unclassified
T014	Cybersecurity Workforce (CSWF) Report	4.4.3 8.1.2 8 2.3.1	MTHLY	30 DATO and monthly on the 10th	Unclassified
T017	Closeout Report	5.2.2 10.3.7	1TIME	NLT 15 days before TO completion date	Unclassified
T008	Contractor CPARS Draft Approval Document (CDAD) Report	5.3	MTHLY	30 DATO and monthly on the 10th	Unclassified
T018	Invoice Support Documentation	5.2.3	ASREQ	Within 24 hrs from request	Unclassified
T019	eCRAFT Report	5.2.4	ASREQ	Same date when invoice is submitted to WAWF	Unclassified

6.1.2 Technical CDRL

The following table lists all required technical data deliverables, (CDRLs), applicable to this task order:

CDRL #	Deliverable Title	PWS Ref Para	Frequency	Date Due	Security Classification (up to S/TS or unclassified)
T003	Monthly Program Review	3.1.2 3.1.3 3.1.4 3.1.5 3.6.2	MTHLY	30 DATO and monthly on the 15th	Unclassified
T005	Requirements Traceability Matrix	3.2.2 3.3 3.4	ASREQ	NLT 10 days after baseline approval	Unclassified

CDRL #	Deliverable Title	PWS Ref Para	Frequency	Date Due	Security Classification (up to S/TS or unclassified)
T020	Release Roadmap	3.2.2 3.3	ONE/R	60 DATO	Unclassified
T006	Architecture Design Artifacts	3.2.3 3.4	ASREQ	Within 10 days after request	Unclassified
T007	Configuration Management Plan	3.2.5	ONE/R	NLT 45 DATO; revision NLT 7 days after receipt of Govt review	Unclassified
T009	Planning Increment Report	3.3	ASREQ	NLT 5 days after completion of Planning Increment	Unclassified
T010	Iteration Review Report	3.3	MTHLY	10th of Each Month for reviews completed during the previous month	Unclassified
T011	Source Code	3.2.6 3.3 3.4 4.3	ASREQ	NLT 10 days after baseline approval	Unclassified
T012	Software Documentation/Programmer's Guide	3.3 3.4 4.3	ASREQ	NLT 10 days after baseline approval	Unclassified
T013	Software Development Plan (SDP)	3.4	ONE/R	30 DATO; revision NLT 7 days after receipt of Govt review	Unclassified
T015	Transition Plan	3.6	2TIMES	NLT 21 DATO NLT 120 days before TO completion date	Unclassified
T016	Data Call Report	5 2.1.2	ASREQ	Within 24-48 hrs after request	Unclassified

6.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail or uploaded to a Government provided electronic repository; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, and etc., are provided in a format

approved by the receiving Government representative. The contractor shall provide all data in an editable format compatible with NIWC Atlantic corporate standard software configuration as specified below. Contractor shall conform to NIWC Atlantic corporate standards within 30 days of task order award. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.*

	Deliverable	**Software to be used**
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher/FrameMaker
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
f.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
g.	Scheduling	Microsoft Project
h.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio
i.	On-line Training Development	Adobe Captivate

6.3 INFORMATION SYSTEM COMMUNICATION

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure (PKI) client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on task shall be accessible by e-mail through individual accounts during all hours. The contractor shall have an information system capable of meeting all security requirements identified under Para 8.4.

7.0 QUALITY

7.1 QUALITY SYSTEM

Upon task order award, the prime contractor shall have and maintain a quality system that meets contract and task order requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The contractor shall have an adequately documented quality system which contains processes, procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system, which includes an internal auditing system. The contractor shall make their quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this task order may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan or quality system, and development of quality related documents. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

(i) Establish documented, capable, and repeatable processes

(ii) Track issues and associated changes needed

(iii) Monitor and control critical process, product, and service variations

(iv) Establish mechanisms for feedback of field product and service performance

(v) Implement and effective root-cause analysis and corrective action system

(vi) Establish methods and procedures and create data used for continuous process improvement

7.2 MANAGE QUALITY COMPLIANCE

7.2.1 General

The contractor shall have quality processes or a Quality Management System (QMS) processes in place that coincide with the Government's Manage Quality processes which address

Quality Control, Quality Assurance, Software Quality, and/or project Quality System tasks. The contractor shall use best industry practices including, when applicable, ISO/IEC/IEEE 15288:2015 for System life cycle processes and ISO/IEC/IEEE 12207:2017 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in Acquisition Milestones, Phases, and Decision Points, which are standard elements of the Defense Acquisition System and support DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment and objective evidence of Lean Six Sigma, Risk Management, and System Engineering methodologies; and System and Software Engineering best practices.

7.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified in the contractor's Quality Assurance Plan (QAP) or by the respective WBS, POA&M, or quality system/QMS documentation in support of continuous improvement. The contractor shall deliver related QAP and any associated procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes, products, and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related products, services, documents, and material in a category when noncompliance is established.

-

7.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified in the contractor QAP or by the respective WBS, POA&M, or quality system/QMS documentation.

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in the DoD Contract Security Classification Specification, DD Form 254, the contractor shall perform classified work under this task order. Prior to commencement of classified work, the contractor shall have a SECRET facility clearance (FCL).

8.1.1.1 U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and work within restricted areas unescorted. Access to SCI is limited to U.S. Government Facilities or other U.S. Government sponsored controlled space as authorized on the DD254. The contractor shall not generate any SCI deliverables.

8.1.1.2 This task order requires for various levels of vetting to support specific PWS tasks. The following table outlines the minimum required security clearance per task. The contractor shall provide personnel meeting the specific minimum personnel clearance (PCL) for access to support the PWS tasks listed below:

Required Security Clearance	**PWS Task Paragraph**
Secret	3.2, 3.3, 3.4, 3.5 & 3.6
None required	3.1

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or access to Government facility/installation and/or access to information technology systems under this task order. The FSO is typically a key management person who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on task order. Responsibilities include tracking all personnel assigned Government Common Access Card (CAC) and NIWC Atlantic badges (issuances and expiration dates) and entering/maintaining personnel security mandatory training information within the Staffing Plan document, which is an attachment to the task order status report (TOSR) (CDRL T001), including updating and tracking data in the CSWF Report (CDRL T014). The FSO shall ensure the latest NIWC Atlantic Contractor Check-in and Check-out (CICO) procedures are implemented and followed.

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30C, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on this task order, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order and are certified/credentialed for the CSWF. A favorable background determination is determined by either a Tier 1 (T1) investigation, Tier 3 (T3) investigation, or Tier 5 (T5) investigation and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or NIWC Atlantic information. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum security requirements, the contractor shall permanently remove the individual from NIWC Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied," receives an "Interim Declination," or unfavorable fingerprint, the contractor shall remove the individual from NIWC Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task orders.

8.2.1 Personnel Clearance

The majority personnel associated with this task order shall possess a SECRET personnel security clearance (PCL). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data to include having access to Naval Nuclear Propulsion Information (NNPI) Data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the DoD CAF and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied as a task order modification. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and NIWC Atlantic security regulations. The contractor shall immediately report any security incident or insider threat indicator to the NIWC Atlantic Security Management Office, the COR, and Government Project Manager.

8.2.1.1 For personnel that require a security clearance, the following labor categories shall meet the designated minimum personnel clearances (PCL) for access:

Labor Category	**Required Minimum Personnel Security Clearance (PCL)**	**TS/SCI Access Required (Y/N)**
Engineer/Scientist Intern	Secret	N
Engineer/Scientist 1	Secret	N
Engineer/Scientist 2	Secret	N
Engineer/Scientist 3	Secret	N
Engineer/Scientist 4	Secret	N
Engineer/Scientist 5	Secret	N
Management Consultant (Senior)	Secret	N
Program Manager	Secret	N
Project Manager	Secret	N
Subject Matter Expert (SME) 1	Secret	N
Subject Matter Expert (SME) 1	Secret	N
Subject Matter Expert (SME) 3	Secret	N
Subject Matter Expert (SME) 4	Secret	N
Subject Matter Expert (SME) 5	Secret	N
Technical Analyst 2	Secret	N
Technical Analyst 3	Secret	N
Technical Analyst 4	Secret	N

8.2.2 Access Control of Contractor Personnel

The contractor shall facilitate the required access for each employee. The ability of the contractor to manage and maintain accessibility in accordance with the applicable requirements is captured in the annual Government CPARS rating.

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government

facility/installation.

(a) The majority of Government facilities/installations require a CAC for access. Contractor personnel shall carry proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement for any liability issues. For admission to NIWC Atlantic facilities/installations, all contractor personnel must have the COR or Government sponsor initiate access. For contractor personnel requiring a Confidential, Secret, or TS security clearance, a visitor authorization request (VAR) must be submitted via Defense Information System for Security (DISS) to the applicable Security Management Office (SMO). The contractor shall send VAR to SMO 652366. For Charleston and other remote locations excluding Tidewater, the contractor shall send VAR to SMO 652366 and for Tidewater locations send VAR to SMO N65580. If faxing a VAR versus using JPAS/DISS, the contractor shall submit their request on company or agency letterhead to (843)218-4045 for SMO 652366 or (757)541-5860 for SMO N65580. For visitation to all other Government locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office.

JPAS is being replaced by DISS. The contractor shall ensure they are capable of accessing DISS when JPAS is no longer accessible. After DISS transition date, contractor shall submit all VARs through DISS.

(b) Contractor employees who make repeated deliveries to JB Charleston military installations and do not require access into NIWC Atlantic facilities or access to IS shall obtain a base access card. Only contractor employees that are able to obtain a card will be eligible for entrance on base. At Joint Base (JB) Charleston, the contractor shall obtain the required access card via the Defense Biometric Identification System (DBIDS) from the JB Charleston Badge and Pass Office. Contractors with employees that that are no longer employed shall return the employee's access card directly to the COR or to the local NIWC Atlantic Security Office with COR notification within five (5) days from the last day of employment. Contractors who do not have a DBIDS card or CAC will receive a one-day pass for each day access is required. Information about DBIDS is found at https://dbids-global.dmdc mil /enroll#!/.

(c) All contractor persons engaged in work while at a Government facility/installation shall be subject to inspection of their vehicles, identification cards, and bags/parcels at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

(d) The contractor shall notify the COR and appropriate NIWC Atlantic security personnel within 24 hours from the time contractor employee gives notice of departure or are removed unexpectedly from contract support. For contractors in direct support of NIWC Atlantic, see the Contractor Check-in and Check-out (CICO) Procedures requirements listed in Para 8.2.2.5.

8.2.2.2 Identification and Disclosure Requirements

All contractor and subcontractor employees located on and off Government installations shall take all means necessary to not represent themselves as Government employees. All contractor personnel shall follow the identification and Government facility disclosure requirement:

(a) Contractor employees shall be clearly identifiable as a contractor while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors shall identify themselves as contractors or subcontractors during meetings, on attendance meeting list/minutes, at the beginning of telephone conversations, in electronic messages including their electronic digital signature, and all correspondence related to this task order.

(c) Contractors occupying facilities within Department of the Navy or other Government installations (such as offices, separate rooms, or cubicles) shall clearly display and identify their space with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

8.2.2.3 Government Badge Requirements

Depending on access required, contractor personnel shall require a Government-issued picture badge. While on Government installations/facilities, contractors shall abide by each site's latest security badge requirements and prominently display (above the waist) their Government-issued picture badge. Government installations/facilities are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards.

(a) Contractors shall submit valid paperwork (e.g., site visit request, request for picture badge, etc.) to the applicable Government security office via the COR who will validate the need authorizing contractor performance within the applicable Government installation/facility.

(b) The contractor shall assume full responsibility for the proper use and security of the identification badge and is responsible for returning the badge upon termination of personnel or expiration or completion of the task order.

(c) The contractor (FSO if applicable) shall track all personnel (including subcontractors) holding CAC and/or NIWC Atlantic Government badges in support of this task as part of the TOSR. At the completion of the task order, the contractor shall provide a list as part of the Closeout Report (CDRL T017) of all returned and unreturned badges with a written explanation for any missing badges.

8.2.2.4 Common Access Card (CAC) Requirements

Contractors supporting work that requires access to Government facilities/installations and/or access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoDM 1000.13-V1, issuance of a CAC is based on the following four criteria:

1. Eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD federally controlled facilities on behalf of the NIWC Atlantic on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the AC logon for user identification.

2. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS).

3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoDM 5200.02 – at a minimum, the completion of FBI fingerprint check with favorable results and submission of a T1 investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. Contractor personnel requiring logical access shall obtain and maintain a favorable T3 investigation. Contractor personnel shall contact the NIWC Atlantic Security Office to obtain the latest CAC requirements and procedures.

4. Verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a PKI. A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the task order specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Atlantic Information Systems Security Management (ISSM) office:

1. For annual DoD Cybersecurity/IA Awareness training, the contractor shall use this site: https://mytwms.dc3n navy.mil/. For contractors requiring initial training and do not have a CAC, contact the NIWC Atlantic ISSM office at phone number (843)218-6152 or e-mail questions to NIWCLANT.ISSM.OPS.FCT@navy.mil for additional instructions. Training can be taken at the ISSM office or online at https://public.cyber.mil/training/cyber-awareness-challenge/.

2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form and shall initiate a CAC request via the latest Contractor Check-in procedures as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website at https://www.public.navy mil/navwar/atlantic/pages /contractorcheckin.aspx.

8.2.2.5 Contractor Check-in and Check-out (CICO) Procedures

All NIWC Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a NIWC Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out (CICO) procedures, instructions, and forms as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website (under “Contact” tab, select “Contractor Check-In”). In accordance with the monthly status reporting requirements, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the CICO instructions. The contractor (FSO, if applicable) shall have IT access to NIWC Atlantic systems for purposes of meeting CICO personnel requirement. For contractor employees whose services are no longer required, the contractor shall ensure all those employees return all applicable Government credentials (keys, CAC, site badges, tokens, etc.) and any assigned Government-furnished property (e.g., laptops) are returned to the COR or appropriate Government representative. The contractor shall ensure all procedures as cited in the Contractor Check-out COG page are followed which includes a completed Contractor Check-out checklist form (SPAWARSYSCEN 5500/3) is submitted for each employee as applicable.

8.2.2.6 Accessing Navy Enterprise Resources Planning (ERP) System

Contractor personnel shall not access the Navy Enterprise Resource Planning (Navy ERP) system.

8.2.3 Mandatory Training

In addition to training requirements and certifications required for a specific labor category, certain contractor personnel (including subcontractors) regardless of security classification shall complete required mandatory training in accordance with NAVWARSYSCOM Code 80330 mandatory training webpage: https://wiki.spawar.navy.mil/confluence/x/jwDsAQ. Mandatory training will be required for contractor personnel (including subcontractors) with access to Naval Nuclear Propulsion Information (NNPI) data. The briefs, user agreement, and training will be required and provided by the US Government for contractors with access to Restricted Data (RD), Formerly Restricted Data (FRD), and NNPI. Contractors without access to the training webpage shall coordinate with the COR concerning the latest mandatory training as specified on the training webpage. The following table is a sample of contractor mandatory training that is subject to change in accordance with the NAVWARSYSCOM website or SECNAVINST:

#	**Training Course Name**	**Contractor Personnel Applicability**
1	Active Shooter, Level 1	All contractors
2	Operations Security (OPSEC)	All contractors
3	Antiterrorism Training, Level 1	Contractors requiring routine physical access to federally controlled facilities or military installations (DFARS 252.204-7004)
4	[NIWC Atlantic] Annual Security Refresher	All fulltime/partial, onsite contractors
5	Suicide Prevention Training (Suicide Awareness)	All fulltime, onsite contractors

6	Records Management	All contractors NMCI account holders
7	DoD Cyber Awareness Challenge	All contractors NMCI account holders and Personnel accessing CAC-enabled gov't sites – Authorized users of DoD information systems and networks
8	Privacy and Personally Identifiable Information (PII) Awareness Training	All contractors with access to PII
9	NIWC Intelligence Oversight	All contractors
10	Sensitive Compartmented Information (SCI) Initial/Refresher Training	Contractors that are SCI cleared personnel and authorized users of DoD IS and networks

8.2.3.1 The contractor shall be responsible for verifying applicable personnel receive all required training within the specified due dates. The contractor shall track and annotate all mandatory training required and completed for each employee in the Staffing Plan which is part of the monthly TOSR (CDRL T001). For CSWF, contractor shall ensure all mandatory cybersecurity training and certifications are reported in the CSWF Report (CDRL T014).

8.2.3.2 Unless otherwise noted, the contractor shall complete mandatory training annually between 1 October and 30 September utilizing the Total Workforce Management System (TWMS). For some personnel, attendance of Government face-to-face training is allowed if COR concurs with training schedule. For training taken via Defense Information Systems Agency / Navy Knowledge Online (DISA/NKO), the contractor shall forward a copy of the certificate to ssclant_mandatory_tr.fcm@navy.milwho will upload or ensure each completed training is recorded in TWMS.

8.2.3.3 The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

8.2.4 Accessing Government Information Systems and Nonpublic Information

Contractor personnel shall meet the following cybersecurity and personnel security requirements when accessing Government information systems and nonpublic information.

Definition – For the purposes of this section, “sensitive information” includes the following:

(a) all types and forms of confidential business information, including financial information relating to a contractor’s pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;

(b) source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 2101-2107);

(c) information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;

(d) other information designated as sensitive by NIWC Atlantic and the program.

8.2.4.1 In the performance of the task order, the contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements.

8.2.4.2 Contractor personnel shall protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the task order, whether the information comes from the Government or from third parties. The contractor shall provide the following support:

(a) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the task order, and not for any other purpose unless authorized;

(b) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the task order or as authorized by Federal statute, law, or regulation;

(c) Inform authorized users requiring access in the performance of the task order regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.

(d) Execute a “Contractor Access to Information Non-Disclosure Agreement,” and obtain and submit to the Contracting Officer a signed “Contractor Employee Access to Information Non-Disclosure Agreement” for each employee prior to assignment.

(e) Notify the Contracting Officer in writing of any violation of the requirements in Para 8.2.4.2(a) through Para 8.2.4.2(d) as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

8.2.4.3 In the event that the contractor inadvertently accesses or receives any information marked as “proprietary,” “procurement sensitive,” or “source selection sensitive,” or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

8.2.4.4 The requirements of this text are in addition to any existing or subsequent OCI requirements which may also be included in the task order, and are in addition to any personnel security or Information Assurance requirements, including SAAR-N form (DD Form 2875), annual Cybersecurity training certificate, Questionnaire for Public Trust form (SF85P), or other forms that may be required for access to Government Information Systems.

8.2.4.5 Subcontracts. The contractor shall insert Para 8.2.4.1 through 8.2.4.4 in all subcontracts that may require access to sensitive information in the performance of the task order.

8.2.4.6 Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the “Contractor Non-Disclosure Agreement,” a mitigation plan for Government approval, which shall be incorporated into the task order. At a minimum, the mitigation plan shall identify the contractor’s plan to implement the requirements of Para 8.2.4.2 and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the task order from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A “firewall” may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

8.2.5 Handling of Personally Identifiable Information (PII)

In accordance with the Privacy Act of 1974, the contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of Personally Identifiable Information (PII) in accordance with the latest DoN policies. The contractor shall not store any Government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in the header and footer of each page of the document: “CUI”. In addition to marking documents at the top and bottom with “CUI” a CUI “Designation Indicator Block” is required at the bottom of the document’s first page within the “CUI” banner and footer markings. DoD guidance directs that this block be located at the lower right of the page. Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Once notified, the Contracting Officer shall immediately contact the Privacy Act Coordinator. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel. If a contractor, including any subcontractor, is authorized access to PII, the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act.

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. OPSEC requirements are applicable when contract personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information. Pursuant to DoDD 5205.02E and SPAWARINST 3432 1, NIWC Atlantic’s OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual and SPAWARSYSCENLANTINST 3070.1B.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall development their own internal OPSEC program specific to the task order and based on NIWC Atlantic OPSEC requirements. At a minimum, the contractor’s program shall identify the current NIWC Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial OPSEC training within 30 days of task order award and annual OPSEC awareness training in accordance with requirements outline in the Mandatory Training, Para 8.2 3. OPSEC training requirements are applicable for personnel during their entire term supporting this NIWC Atlantic task order.

8.3.3 NIWC Atlantic OPSEC Program

Contractor shall participate in NIWC Atlantic OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified task order shall have specific OPSEC requirements listed on the DD Form 254.

8.4 INFORMATION SYSTEM SECURITY

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on task. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the task order, and privileged task order information (e.g., program schedules and task order-related tracking).

8.4.1 Hardware and Software

The contractor shall scan all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect task order related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure Data-at-Rest encryption technology is installed on all portable electronic devices including storage of all types.

8.4.2 Safeguards

The contractor shall protect Government information and shall be able to provide documentation (e.g , Systems Security Plan (SSP)) validating they are complying with the requirement in accordance with DFARS 252 204-7012. Subcontractors are subject to DFARS requirements only when performance will involve operationally critical support or covered defense information. The contractor and all applicable subcontractors shall abide by the following safeguards:

8.4.2.1 Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

8.4.2.2 Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

8.4.2.3 Sanitize media (e.g., overwrite, reformat, or degauss) before external release or disposal.

8.4.2.4 Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

8.4.2.5 Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

8.4.2.6 Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption. The contractor shall encrypt or digitally sign all communications for authentication and non-repudiation.

8.4.2.7 Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

8.4.2.8 Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

8.4.2.9 Provide protection against computer network intrusions and data exfiltration, minimally including the following:

(a) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

(b) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(c) Prompt application of security-relevant software patches, service packs, and hot fixes.

8.4.2.10 As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

8.4.2.11 Report loss or unauthorized disclosure of information in accordance with contract, task order, or agreement requirements and mechanisms.

8.4.2.12 Pursuant to DFARS 252.204-7009, the contractor shall not use or disclose third-party contractor reported cyber incident information. The contractor can be held liable for breach of information and shall extend restriction in subcontracts for service that include support to Government's activities related to safeguarding covered defense information and cyber incident reporting.

8.4.2.13 As applicable, follow minimum standard in SECNAVINST 5510 36B for classifying, safeguarding, transmitting, and destroying classified information and CUI.

8.4.3 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

8.4.4 Covered Defense Information

The contractor shall identify all covered defense information, as defined in DFARS 252.204-7012, and apply markings when appropriate to all deliverables in accordance with DoDI 5200.48.

8.4.5 Utilization of a Government-owned and Government-controlled computer asset

The contractor shall meet specific operational requirements when utilizing a Government-owned computer or Government-controlled software image for a contractor-owned computer (including laptop) that is issued as either an NMCI asset, Government Furnished Property (GFP), or Government Controlled Equipment (GCE). At a minimum, contractor personnel shall comply with the following requirements when utilizing a Government-owned or Government-controlled computer:

8.4.5.1 All messages sent to/from utilize VPN connections.

8.4.5.2 All messages sent to/from are encrypted.

8.4.5.3 No storage of data on non-compliant networks (e.g., contractor's corporate systems).

8.4.5.4 Only government email (NMCI, mail.mil, etc.) is allowed to be used; absolutely NO Gmail, other personal systems, and NO corporate email that does not reside on NIST compliant systems shall be utilized.

8.4.5.5 All email must be sent between compliant systems – e.g., sending encrypted email to a private corporate account that resides on an uncompliant network, then decrypting and utilizing it is not allowed.

8.4.5.6 All stored information meets data-at-rest encryption standards – if using GFP, then use the same methods as networked devices (e.g., MS Bitlocker, Symantec Endpoint Security, etc.)

8.4.5.7 All data is housed on GFE shared storage location – ensures government can retrieve its data at any time.

8.4.5.8 In regard to processing, storing or transmitting CUI, no CUI is allowed on an information system not meeting configuration and security standards.

8.5 ENHANCED SECURITY CONTROLS

Controlled unclassified information (CUI), as defined in DoDI 5200.48, is applicable to this contract. Pursuant to DFARS 252.204-7012, prior to the processing, storing, or transmitting of CUI on an unclassified information system and IT asset that is owned, or operated by or for the contractor, the contractor shall meet the following enhanced security controls.

8.5.1 Systems Security Plan and Plan of Action and Milestones (SSP/POA&M) Reviews

8.5.1.1 Within thirty (30) days of task order award, the contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in DFARS 252.204-7012, which is included in this task order. The contractor shall

fully cooperate in the Government's review of the SSPs at the contractor's facility.

8.5.1.2 If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS 252.204-7012 then the Government will notify the contractor of each identified deficiency. The contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The Contracting Officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the contractor to submit a plan of action and milestones (POA&M) for the correction of the identified deficiencies. The contractor shall immediately notify the Contracting Officer of any failure or anticipated failure to meet a milestone and provide an updated POA&M.

8.5.1.3 Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the contractor's facility. The Government may continue to conduct follow-on reviews until the Government determines that the contractor has corrected all identified deficiencies in the SSP(s).

8.5.1.4 The Government may, in its sole discretion, conduct subsequent reviews at the contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of task order award) and may conduct such reviews at any time upon thirty (30) days' notice to the contractor.

8.5.2 Compliance to NIST 800-171

8.5.2.1 The contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&M that varies from NIST 800-171 only in accordance with DFARS 252.204-7012(b)(2), for all covered contractor information systems affecting this task order.

8.5.2.2 Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

(a) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as Computer Numerical Control (CNC) equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

(b) Implement Control 3.1 5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

(c) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods;

(d) Audit user privileges on at least an annual basis;

(e) Implement:

1. Control 3.13.11 (FIPS PUB 140-2 validated cryptology or implementation of National Security Agency (NSA) or NIST approved algorithms (i.e. FIPS PUB 140-2 Annex A: Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) or compensating controls as documented in a SSP and POA&M); and,

2. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

(f) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POA&M for implementation which shall be evaluated by the Navy for risk acceptance;

(g) Implement Control 3 1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program

8.5.3 Cyber Incident Response

8.5.3.1 The contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the task order that the contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

8.5.3.2 Incident data shall be delivered in accordance with the DOD Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

8.5.3.3 If the contractor subsequently identifies any such data not previously delivered to DC3, then the contractor shall immediately notify the Contracting Officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the contractor may request a delivery date later than ten (10) days after identification. The Contracting Officer will approve or disapprove the request after coordination with DC3.

8.5.4 Naval Criminal Investigative Service (NCIS) Outreach

The contractor shall engage with Naval Criminal Investigative Service (NCIS) industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

8.5.5 NCIS/Industry Monitoring

8.5.5.1 In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the contractor shall cooperate with the NCIS, which may include cooperation related to: threat indicators; pre-determined incident information derived from the contractor's infrastructure systems; and the continuous provision of all contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

8.5.5.2 If the Government determines that the collection of all logs does not adequately protect its interests, the contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the contractor. In the alternative, the contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the contractor.

8.5.5.3 In all cases, the collection or provision of data and any activities associated with this PWS shall be in accordance with federal, state, and non-US law.

9.0 GOVERNMENT FURNISHED INFORMATION (GFI)

For the purposes of this task order, Government Furnished Information (GFI) includes manuals, technical specifications, software, software licenses, maps, building designs, schedules, drawings, test data, etc. provided to contractors for performance on this task order. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution. The Government will mark any CUI which includes unclassified covered defense information and unclassified controlled technical information provided to the contractor. For any missing markings, contractor shall request appropriate marking from the Government.

GFI is utilized on this task order. Any applicable document (PWS Para 16.0) not available online, the Government will provide document as GFI listed in the table below. The contractor shall inventory all GFI by tracking distribution and location and provide a GFI inventory to the Government. The contractor shall use the GFI provided to support this task order only – use of GFI document(s) to support other projects beyond this task order is not allowed. Unless otherwise specified, all GFI will be provided by the Government by the estimated delivery date listed in the table below, and the contractor shall return all GFI to the Government at completion of the task order. If a contractor requires additional GFI other than what is listed, the contractor shall submit a written request to the COR within 30 days after task order award.

Item #	Description	GFI Estimated Delivery Date
1	Government Software Development Life Cycle (SDLC) Guide	14 days after task order award
2	Government Project Management Plan	14 days after task order award
3	Microsoft Visual Studio	14 days after task order award
4	Enterprise Architect	14 days after task order award
5	Toad	14 days after task order award
6	Access to Government Development Security and Operations Environments and tooling	Request for access 14 days after task order award

10.0 GOVERNMENT PROPERTY

As defined in FAR Part 45, Government property is property owned or leased by the Government which includes Government-furnished property (GFP) and Contractor-acquired property (CAP). Government property is material, equipment, special tooling, special test equipment, and real property.

GFP will not be provided and CAP is not anticipated on this task order.

NOTE: NMCI computers will be assigned to a contractor. Prior to a NMCI computer being removed from a Government facility, the contractor employee shall possess at all times a Property Pass (OF-7) with each NMCI asset that will be authorized and signed by the COR or other authorized Government personnel. Although NMCI assets are not tracked as GFP, the contractor shall separately track and report all NMCI assets assigned to all contractor employees for use on this task order. For reporting purposes, the contractor shall include a list of NMCI assets assigned to this task order (separate from the GFP inventory list) in the TOSR (CDRL T001)

11.0 TRAVEL

11.1 LOCATIONS

The contractor shall be prepared to travel to all the locations listed within this section. Contractor personnel traveling in support of DoD shall travel in accordance with the latest Joint Travel Regulations (JTR) at time travel is being performed. The contractor shall comply with travel cost pursuant to FAR 31.205-46. The contractor shall notify the COR prior to traveling to ensure Government coordination.

Exact travel dates are not known at time of task order award, and locations are subject to change. The proposed travel locations identified are based on historical data.

TRAVEL IS FOR BASE YEAR AND EACH OPTION YEAR, IF EXERCISED

# Trips	# People	# Days/Nights	From (Location)	To (Location)
4	3	5/4	Norfolk, VA	San Diego, CA
4	3	5/4	Norfolk, VA	New Orleans, LA
4	3	5/4	Norfolk, VA	Charleston, SC

12.0 SAFETY ISSUES

12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the task orders. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system. If performing within Government facilities, contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the COR or on-site Government representative.

13.0 SUBCONTRACTING REQUIREMENTS

If the prime contractor is planning to utilize subcontractor(s) on this task order, the prime contractor shall identify the applicable subcontractor(s) in its proposal for the task order. Should the prime contractor be awarded a task order, only those subcontractors included in the proposal upon which the award is based are approved for use on the task order. Post award subcontractor additions (i.e. subcontractor additions to a task order after issuance of the order) are governed by FAR 52.244-2.

In addition, while Government consent to subcontract is not required for prime contractors with an approved purchasing system, if after award of a task order the prime contractor intends to enter into a subcontract with an entity not identified in its proposal upon which the task order award was based, the prime contractor shall nevertheless notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of the task order. Such notification shall include, (i) a description of the supplies or services to be subcontracted, (ii) identification of the subcontract type to be used, (iii) identification of the proposed subcontractor, and (iv) the proposed subcontract price.

13.1 AUTHORIZED SUBCONTRACTORS

The following subcontractor(s) is either identified by the contractor at the time of award of the task order, have been consented to by the Government pursuant to the Subcontracts clause of the contract, or, in the event the contractor has an approved purchasing system, the contractor has provided notification in accordance with paragraph 13.0 above:

(b) (4)

14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the QASP, Attachment 1.

15.0 OTHER CONDITIONS/REQUIREMENTS

15.1 WORKWEEK

All or a portion of the effort under this task order will be performed on a Government installation. The contractor shall provide support services corresponding to Government workweek and core hours. Normal workweek is Monday through Friday. Normal business hours occur 0730-1600 local standard time (LST) based on location of work. Pursuant to Federal law (5 U.S.C. 6103), the Government observes the following public holidays per year. For planning purposes, contractors working in Government spaces shall treat these holidays as Government non-work days which may affect accessibility to Government space.

Name of Holiday	Time of Observance
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February

Memorial Day	Last Monday in May
Juneteenth	19 June
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday will be observed by the Government on the prior Friday or following Monday, respectively.

15.2 EXTENDED WORK WEEK

Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended work week (EWW) may be required for professional (i.e., salaried) employees.

16.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

The contractor shall ensure all work accomplished utilizes the latest, relevant industry practices and standards when applicable unless otherwise indicated by text. In accordance with Defense Acquisition Policy, maximum utilization of non-Government standards will be made wherever practical.

16.1 REQUIRED DOCUMENTS

The contractor shall utilize the following mandatory documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the contractor shall meet requirements for any referenced document including subsequent updates applicable at time the task order request for proposal is posted.

	Document Number	**Title**
a.	DoDM 5200.01	DoD Manual – Information Security Program (vol 1, 2, 3) dtd 24 Feb 12 with Change 2/4/3 dtd 28 Jul 20
b.	DoDM 5200.02	DoD Manual – Procedures for the DoD Personnel Security Program dtd 3 Apr 17
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12 with Change 2 dtd 20 Aug 20
d.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08 with Change 1 dtd 26 Apr 18
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06 with Change 2 dtd 18 May 16
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program (NISP) dtd 18 Mar 11 with Change 2 dtd 24 Sep 20
g.	DoDI 5200.48	DoD Instruction – Controlled Unclassified Information (CUI) dtd 6 Mar 20
h.	DoDD 8140.01	DoD Directive – Cyberspace Workforce Management dtd 05 Oct 20
i.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14 with Change 1 dtd 07 Oct 19
j.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14 with Change 2 dtd 28 Jul 17
k.	DoD 8570.01-M	DoD Manual – Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 (and subsequent replacement)
l.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 22 Feb 16

	Document Number	Title
m.	SECNAV M-5239.2	Secretary of the Navy Manual – DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual dtd June 2016 (and subsequent revisions)
n.	SECNAVINST 5239.3C	Secretary of the Navy Instruction – DoN Cybersecurity Policy dtd 2 May 16
o.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DoN Cyberspace IT and Cybersecurity Workforce Management and Qualification dtd 10 Feb 16
p.	SECNAVINST 5510.30C	Secretary of the Navy Instruction – DoN Personnel Security Program (PSP) Instruction dtd 6 Oct 06
q.	SECNAVINST 5510.36B	Secretary of the Navy Instruction – DoN Information Security Program dtd 12 Jul 19
r.	SPAWARINST 3432.1	Space and Naval Warfare Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
s.	SPAWARSYSCENLANTINST 3070.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Operations Security Policy dtd 20 Jan 17
t.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR) - Navy
u.	JTR	The Joint Travel Regulations (JTR) – Uniformed Service Members and DoD Civilian Employees
v.	NIST SP 800-171	National Institute of Standards and Technologies (NIST) Special Publication (SP)
w.	Section 508 of the Rehabilitation Act of 1973	United States federal law, as amended, 29 U.S.C. § 794d
x.	Privacy Act of 1974	United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a

16.2 GUIDANCE DOCUMENTS

The contractor shall utilize the following guidance documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the document's effective date of issue is the task order's request for proposal issue date.

	Document Number	Title
a.	DoDM 1000.13-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, Volume 1, dtd 23 Jan 14
b.	DoDD 5000.01	DoD Directive – The Defense Acquisition System dtd 20 Nov 07
c.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System dtd 7 Jan 15
d.	NAVSEA TS 9090-310G	NAVSEA Technical Specification: Alterations to Ships Accomplished by Alteration Installation Teams, 9090-310G dtd 12 Feb 15 (and subsequent revisions)
e.	OSHA Public Law 91-596	Compliance with OSHA Standard 29 CFR 1910, 1915, and 1926
f.	ISO/IEC/IEEE 12207:2017	International Organization for Standardization/ International ElectrotechnicalCommission/Institute of Electrical and Electronics Engineers: Systems and Software Engineering – Software Life Cycle Processes
g.	ISO/IEC/IEEE 15288:2015	International Organization for Standardization/ International ElectrotechnicalCommission/Institute of Electrical and Electronics Engineers: Systems and Software Engineering – System Life Cycle Processes

	Document Number	Title
h.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors dtd 27 Aug 04
i.	FIPS PUB 140-2	NIST Security Requirements for Hardware & Software https://csrc.nist.gov/publications/detail/fips/140/2/final
j.	FIPS PUB 140-2 Annex A	Approved List of Security Functions
k.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
l.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
m.	N/A	NIWC Atlantic Public website – CICO Procedures https://www.public navy.mil/navwar/atlantic/pages /contractorcheckin.aspx
n.	N/A	NIWC Atlantic COG page – Procurement Role ERP https://wiki.spawar.navy.mil/confluence/x/uQGRBg
o.	N/A	NAVWARSYSCOM Code 80330 mandatory training webpage – https://wiki.spawar.navy.mil/confluence/x/jwDsAQ

16.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents necessary for performance on this task order. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO , Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization’s website.

[END OF PWS]